

UNITED STATES DISTRICT COURT

for the
Southern District of OhioFILED
RICHARD W. HASEL
CLERK OF COURT

2017 FEB 23 PM 2:03

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Information associated with the Dropbox account
bigblue8992@gmail.com that is stored at premises
controlled by Dropbox Inc.

Case No.

3:17mj 067

MICHAEL J. NEWMAN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment Alocated in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

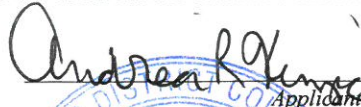
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

See Attachment C

Offense Description

The application is based on these facts:
See Attached Affidavit☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

 Applicant's signature
Andrea R. Kinzig, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date:

2/23/17

City and state: Dayton, Ohio


 Judge's signature
Michael J. Newman, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

Information associated with the Dropbox account bigblue8992@gmail.com that is stored at premises owned, maintained, controlled, or operated by Dropbox Inc., a company that accepts service of legal process at 185 Berry Street, Suite 400, San Francisco, California, 94107.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Dropbox Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All available user/subscriber details for the account, including: full name, user identification number, birth date, gender, contact e-mail addresses, passwords, security questions and answers, telephone numbers, screen names, websites, and other personal identifiers;
- b. All files downloaded and/or uploaded by the user account, including any deleted files;
- c. All activity logs for the account, including but not limited to auth.txt logs, uploag.html files, report.txt files, links.txt files, and any logs reflecting the deletion of files;
- d. Records of any Dropbox links posted by the account user, and records of any other users who accessed these links;
- e. Records of any Dropbox links accessed by the account user, and records of the original poster of those links;
- f. All information related to the account’s settings, including but not limited to linked devices, linked Facebook and Twitter accounts, etc.;
- g. The length of service (including start date);
- h. Any payment information related to the account, including full credit card numbers.

Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, Dropbox Inc. shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of offenses involving receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2)(B) & (b)(1) and 2252A(a)(2); and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) & (b)(2) and 2252A(a)(5)(B), involving the user of the account and occurring from January 1, 2016 to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following:

- a. Any visual depictions and records related to the possession, receipt, and distribution of child pornography;
- b. Any visual depictions of minors;
- c. Records of child pornography files shared with and received from other users, including the identities of those users;
- d. Records of dates and times that files were posted to and accessed by the account user;
- e. Evidence of utilization of other email accounts, social media accounts, online chat programs, and file storage accounts, including any account or user names;
- f. Evidence of utilization of any electronic devices or computer media;
- g. Any information regarding utilization of websites and social media sites to access or obtain child pornography, communicate with juveniles, or communicate with others regarding child exploitation offenses;
- h. Evidence of utilization of aliases and fictitious names;
- i. Any information related to Internet Protocol (IP) addresses accessed by the account;
- j. Information relating to who created, used, or communicated with the account.

ATTACHMENT C

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2)	Receipt and Distribution of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review thousands of examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents and investigators of the FBI, I am currently involved in an investigation of child pornography offenses committed by an individual utilizing accounts associated with the email addresses bigblue8992@yahoo.com and bigblue8992@gmail.com. This Affidavit is submitted in support of an Application for a search warrant for the following:
 - a. Information associated with the Dropbox account bigblue8992@gmail.com that is stored at premises controlled by Dropbox Inc. (as more fully described in Attachment A).
3. The purpose of the Application is to seize evidence of the following violations: receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2)(B) & (b)(1) and 2252A(a)(2); and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) & (b)(2) and 2252A(a)(5)(B). The items to be searched for and seized are described more particularly in Attachment B hereto.
4. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
5. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the search of the above noted account (as described in Attachment A).
6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§ 2252(a)(2)(B) & (b)(1), 2252A(a)(2), 2252(a)(4)(B) & (b)(2), and

2252A(a)(5)(B), are present within the information associated with the above noted account (as described in Attachment A).

PERTINENT FEDERAL CRIMINAL STATUTES

7. 18 U.S.C. § 2252(a)(2)(B) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mail if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
8. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
9. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
10. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
11. For purposes of the statutes, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2) as:
 - a. “Actual or simulated –

- i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
- ii. Bestiality;
- iii. Masturbation;
- iv. Sadistic or masochistic abuse; or
- v. Lascivious exhibition of genitals or pubic area of any person.”

BACKGROUND INFORMATION

Definitions

12. The following definitions apply to this Affidavit and Attachment B to this Affidavit:
- a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
 - b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
 - c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
 - d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
 - e. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can

establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

- f. An “**Internet Protocol address**”, also referred to as an “**IP address**”, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
- g. A network “**server**,” also referred to as a “**host**,” is a computer system that has been designated to run a specific server application or applications and provide requested services to a “client” computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.
- h. A “**client**” is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and retrieve web pages for display. E-mail clients (like Microsoft Outlook or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.
- i. “**Domain Name**” refers to the common, easy to remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically “.com” for commercial organizations, “.gov” for the governmental organizations, “.org” for organizations, and “.edu” for educational organizations. Second level names will further identify the organization, for example “usdoj.gov” further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The

Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as “www.usdoj.gov,” to its currently assigned IP address (*i.e.*, 149.101.1.32), to enable the follow of traffic across the Internet.

- j. **“Log Files”** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.
- k. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- l. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- m. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- n. The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic

notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Characteristics of Child Pornographers

13. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):
 - a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
 - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
 - c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
 - d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.
 - e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Use of Computers and the Internet with Child Pornography

- 14. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production; communication; distribution and storage.
 - a. **Production:** Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited (*i.e.*, lightened, darkened, cropped, digitally enhanced, *etc.*) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.
 - b. **Communication.** Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or "IM"), and individuals may then establish one-on-one chat sessions involving private messages (or "PMs"), visible only to the two parties, to trade child pornography. These child pornography images may be attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to engage in mutual validation of their interest in such material through Internet-based communications.

- c. **Distribution.** Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.
- d. **Storage.** The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage of these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

Google Services

- 15. Google Inc. is a multi-national corporation with its headquarters located in Mountain View, California. The company specializes in Internet-related products and services, including an Internet search engine (www.google.com), productivity tools such as email service (gmail), and enterprise products such as Google Search Appliance.
- 16. Google Photos is a photograph and video sharing and storage service provided by Google Inc., located at photos.google.com. It allows users to back-up their photographs and videos so they can be accessed on any phone, tablet, or computer. It also allows users to pool their photographs and videos together with others into shared albums. Photographs and videos can be organized and searched by places and things in them.
- 17. Google+ is a social networking and identity service website owned and operated by Google Inc., located at www.plus.google.com. Common features include the following:
 - a. **Profiles:** Users can establish profile pages to maintain personal information, similar to the Facebook and MySpace social networking sites.
 - b. **Circles:** Google+ allows users to establish "circles", which enables them to organize people into groups for sharing across various Google products and

services. This service replaces the typical “Friends” list function used by sites such as Facebook and MySpace.

- c. Communities: Communities allow users with common interests to communicate with each other.
 - d. Photos: Google+ allows users to post, back-up, and share photographs. Users can also make comments on photographs posted by other users.
 - e. Hangouts: Hangouts are places used to facilitate group video chat. Only Google+ users can join such chats.
 - f. Messenger: Messenger is a feature available to Android, iPhone, and SMS devices for communicating through instant messaging within Circles.
18. Google Web and App History is a feature of Google Search in which a user’s search queries and results and activities on other Google services are recorded. The feature is only available for users logged into a Google account. A user’s Web and App History is used to personalize search results with the help of Google Personalized Search and Google Now.

Cloud Storage and Dropbox

19. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations. The following terms relate to the use of cloud computing:
- a. “Cloud” is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. “The cloud” was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a network, often the Internet. However, cloud computing offers specific services whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.
 - b. “Cloud computing” is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- c. “Cloud Service Provider” (CSP) is the entity that offers cloud computing services. CSP’s offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual machines, or Web hosting. Service is billed as a utility based on usage. CSP’s maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSP’s reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long- term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as “electronic storage,” and the provider of such a service is an “electronic communications service” provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a “remote computing service.” CSP’s may be able to provide some of the following, depending on the type of services they provide: NetFlow, Full Packet Captures, Firewall and Router Logs, Intrusion Detection Logs, Virtual Machines, Customer Account Registration, Customer Billing Information.
 - d. “Virtual Machine” (VM) is a system where the hardware is virtual rather than physical. Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a VM, does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.
 - e. “NetFlow Records” are collections of network statistics collected by a service provider about traffic flows. A traffic flow is a sequence of data packets from a source to a destination. NetFlow is collected when it is impractical to collect all of the data packets for a flow. Providers may use these logs for quality control, security, or billing. For any particular network flow, NetFlow can include the source and destination IP addresses, network ports, timestamps, and amount of traffic transferred. A provider may only collect a sample of all possible sessions, and may only store the NetFlow for a short time.
20. Dropbox is an on-line service that allows its users to store files on Dropbox Inc.’s servers. According to Dropbox Inc.’s privacy policy, at <https://www.dropbox.com/privacy>, Dropbox Inc. collects and stores “the files you upload, download, or access with the Dropbox Service,” and also collects logs: “When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device’s IP address, browser type, the web page visited before you came to our website, information you search for on

our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your Files, and other interactions with the Service.

21. In general, providers like Dropbox Inc. ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the IP addresses used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.
22. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

Background on NCMEC

23. The National Center for Missing and Exploited Children (commonly known as "NCMEC") was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.
24. As part of its functions, NCMEC administers the CyberTipline. The CyberTipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the CyberTipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities.

BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE

25. On or around September 15, 2016, an anonymous citizen reported to NCMEC's CyberTipline that child pornography was located at the following URL:
<https://www.dropbox.com/sh/zdvr4evmkaenkj/AABC7UPVDMl5eztCvrnyyDzSA?dl=0>

- . A CyberTipline report was prepared and forwarded to the FBI for further investigation.
26. On or around September 21, 2016, an FBI analyst accessed the aforesaid URL and found that it contained approximately thirty-seven image files, some of which contained child pornography. The analyst downloaded the thirty-seven files and provided them to me for further review. Based on my training and experience, I believe that at least approximately fifteen of the files depict images of child pornography (as defined by 18 U.S.C. § 2256). Two of the files are described as follows:
- a. 5393e6e9-13f0-4789-9422-a3029f0d43dd.jpg: This file is an image that depicts a pre-pubescent white female child who is completely nude. The child is squatting over an object that is inserted into her vagina.
 - b. 63337ca7-6610-4b98-be23-963184cc94b5.jpg: This file is an image that depicts the groin area of what appears to be an infant white female child. The penis of what appears to be an adult white male is touching the child's nude vagina.
27. On or around September 21, 2016, an administrative subpoena was served on Dropbox Inc. requesting information associated with the aforesaid Dropbox URL. Records provided by Dropbox Inc. in response to this subpoena identified that the URL belonged to a Dropbox account held in the name of "Jay Bigs", with a log-in email address of bigblue8992@yahoo.com. Dropbox Inc.'s records further indicated that the user had established the account on or around June 30, 2016. Dropbox Inc.'s records also identified that the account had been logged into on two separate occasions – that being on June 30, 2016 and September 1, 2016. According to Dropbox Inc.'s records, the IP address of 50.5.114.147 was utilized to log into the account on both occasions.
28. On or around October 4, 2016, Dropbox Inc. reported to NCMEC's CyberTipline that approximately fifteen image files and approximately six video files containing suspected child pornography were discovered in the publicly available content of the Dropbox account with an account name of "Jay Bigs" and with a log-in email address of bigblue8992@yahoo.com (the same account noted above that contains the aforesaid URL). Dropbox Inc. provided NCMEC with the twenty-one image and video files as well as an upload log, which detailed the dates, times, and file names of all files uploaded to the account. The files and upload log were forwarded to the FBI for further investigation.
29. I have reviewed the twenty-one files provided by Dropbox Inc. I noted that many of these files were also found in the files downloaded by the FBI analyst on or around September 21, 2016, including the two image files described in paragraph 39. Based on my training and experience, I believe that at least fifteen of the image files and at least six of the video files depict child pornography (as defined by 18 U.S.C. § 2256). One of the files is described as follows:
- a. 5e12d91e-9e45-4ee1-8bdc-b078ddd00440.mp4: This file is a video that depicts two pre-pubescent female children, one of which is nude and the other of which is

wearing clothing. The child who is wearing clothing is inserting an object into the vagina of the nude child. The video is approximately thirty-one seconds in duration.

30. I have also reviewed the upload log provided by Dropbox Inc. and noted that more than nine hundred files were uploaded to the account between the approximate time period of July 14, 2016 and August 31, 2016. As such, it appears that there were more files in the account than those which Dropbox Inc. provided to NCMEC.
31. Cincinnati Bell was identified as being the Internet Service Provider of the IP address 50.5.114.147 (the IP address utilized to log into the bigblue8992@yahoo.com Dropbox account, as detailed above). On or around October 24, 2016, an administrative subpoena was served on Cincinnati Bell requesting subscriber information for this IP address on the aforesaid two dates and times it was used to log into the subject Dropbox account. Records provided by Cincinnati Bell in response to the subpoena identified that this account was subscribed to by a Lois Bigler at 104 Virginia Avenue in Dayton, Ohio. Lois Bigler's Internet account was created on or around May 7, 2016, and remained active as of the date of the subpoena.
32. On or around December 29, 2016, an administrative subpoena was served on Yahoo Inc. requesting information for the bigblue8992@yahoo.com email account. Records provided by Yahoo Inc. in response to the subpoena identified that the account was created on or around March 1, 2015, and that the user identified his name as being "J Big" (which is similar to the "Jay Bigs" name associated with the bigblue8992@yahoo.com Dropbox account). The user also provided a telephone number of 937-304-4995 as an alternate communication channel. Logs of IP addresses identified that this account was logged into on approximately twenty-six separate occasions between the approximate time period of April 2, 2016 and October 18, 2016. On approximately twenty of these occasions, the IP address of 50.5.114.147 (the IP address utilized to log into the Dropbox account and that is subscribed to Lois Bigler at 104 Virginia Avenue in Dayton, Ohio, as detailed above) was utilized to log into the account.
33. Sprint Corporation was identified as being the service provider for telephone number 937-304-4995. On or around January 6, 2017, an administrative subpoena was served on Sprint Corporation requesting subscriber and transactional information for the phone number for the time period of July 1, 2016 to January 6, 2017. Records received from Sprint Corporation in response to the subpoena identified that this account was subscribed to in the name of Lois Bigler, with a billing address of 104 Virginia Avenue in Dayton, Ohio. Records also identified that the telephone associated with the account had accessed Internet data on approximately thirty-three occasions between the approximate time period of October 28, 2016 and January 30, 2017.
34. On or around February 6, 2017, an administrative subpoena was served to Google, Inc. requesting information for any Google accounts associated with the email address bigblue8992@yahoo.com. Records provided by Google Inc. in response to the subpoena identified that the bigblue8992@yahoo.com email address was associated with a Google

account using the email address bigblue8992@gmail.com. The bigblue8992@gmail.com Google account was created on or around April 6, 2015. When opening the account, the user identified that his name was "A Big", his telephone number was 937-304-4995, and his recovery email address was bigblue8992@yahoo.com.

35. According to Google Inc.'s records, services utilized by the bigblue8992@gmail.com included the following: Gmail, Google Photos, Google+, and Web & App Activity. Also according to Google Inc.'s records, the account was logged into on approximately seven occasions between the approximate time period of September 22, 2016 and November 23, 2016. On each of these seven occasions, the IP address of 50.5.114.147 (the IP address utilized to log into the Dropbox and Yahoo email accounts and that is subscribed to Lois Bigler at 104 Virginia Avenue in Dayton, Ohio, as detailed above) was utilized to log into the account.
36. Based on review of prior FBI case reports, I have determined that Lois Bigler is approximately seventy-four years of age and is the mother of Jason Bigler. Jason Bigler is currently required to register as a sex offender as a result of the following prior convictions:
 - a. In May 2002, Jason Bigler was convicted in the Van Wert County (Ohio) Common Pleas Court of one count of unlawful sexual conduct with a minor, in violation of Ohio Revised Code Section 2907.04(a). Jason Bigler was sentenced to two years imprisonment.
 - b. In June 2007, Jason Bigler was convicted in the United States District Court for the Southern District of Ohio of one count of possession of child pornography, in violation of 18 U.S.C. §2252(a)(4)(b) & (b). Jason Bigler was sentenced to 120 months imprisonment and lifetime supervised release.
37. A review of Jason Bigler's criminal history identified that in addition to the above-noted convictions, he was also arrested by the Grove City (Ohio) Police Department in September 2000 for rape, in violation of Ohio Revised Code Section 2902.02. Records from the Grove City Police Department identified that a 14-year old female child reported that Jason Bigler had engaged in sexually explicit conduct with her after meeting her on the Internet. The child further reported that when they first began communicating with each other, Jason Bigler represented himself as being 16 years old. The criminal charges were later dismissed.
38. Based on records from the Adult Parole Authority of the Ohio Department of Rehabilitations and Corrections, I have determined that Jason Bigler's aforesaid 2002 conviction in Van Wert County resulted from an investigation conducted by the Delphos (Ohio) Police Department. According the records, Jason Bigler traveled to the City of Delphos to engage in sexually explicit conduct with a 14-year old girl who he met on a teen Internet chat line and who he communicated with via the Yahoo messenger application.

39. Based on records obtained from prior FBI case reports, I have determined that Jason Bigler's aforesaid 2007 conviction in the United States District Court for the Southern District of Ohio resulted from an investigation conducted by the FBI and Adult Parole Authority. Records identified that after Jason Bigler was released from prison for his 2002 conviction and while he was serving a term of parole, Parole Officers found him in possession of various computer media. Possessing this computer media was a violation of his parole conditions, and the computer media were seized and examined. The examination recovered approximately 190 images and approximately 12 videos of child pornography.
40. Jason Bigler was released from federal prison on or around December 2, 2014, and he is presently serving his term of lifetime supervised release. He is currently supervised by Probation Officer (PO) Christopher Owens of the United States Probation Service in Dayton, Ohio. As part of the conditions of his supervised release, Jason Bigler is prohibited from possessing or using a computer or any device with access to any "on-line computer service" at any location without prior written approval of his probation officer. PO Owens has not provided such approval to Jason Bigler. As such, Jason Bigler is prohibited from having email and Dropbox accounts and accessing Internet data from his cellular telephone.
41. Jason Bigler has reported to PO Owens that he resides at 105 Virginia Avenue in Dayton, Ohio. PO Owens' records indicate that Jason Bigler began living at this address in or around January 2015. As part of his sex offender registration requirements, Jason Bigler has also reported to the Montgomery County (Ohio) Sheriff's Office that he resides at 105 Virginia Avenue in Dayton, Ohio.
42. Pursuant to the terms of Jason Bigler's supervised release, PO Owens has conducted multiple home visits at 105 Virginia Avenue in Dayton, Ohio. PO Owens conducted a home visit as recently as February 2, 2017, and verified that Jason Bigler continues to reside at the residence.
43. Jason Bigler has told PO Owens that his telephone number is 937-304-4995 (the telephone number noted in the subscriber information for the bigblue8992@yahoo.com and bigblue8992@gmail.com email accounts, as detailed above). PO Owens has communicated with Jason Bigler via this telephone number as recently as January 31, 2017.
44. Jason Bigler has reported to PO Owens that he drives a 2000 Saturn SL1 bearing Ohio license plate AXN4197, silver in color. During previous home visits, PO Owens has seen Jason Bigler drive the Saturn and/or has seen the vehicle parked in front of or near the residence at 105 Virginia Avenue.
45. I have determined that Jason Bigler's residence at 105 Virginia Avenue in Dayton, Ohio is located directly across the street from Lois Bigler's residence at 104 Virginia Avenue in Dayton, Ohio (where Internet Service is received via Cincinnati Bell). Based on my

training and experience, I know that Internet service for a residence can often be accessed from neighboring residences. Based on the proximity of the two residences located at 104 Virginia Avenue and 105 Virginia Avenue, Jason Bigler could likely access Lois Bigler's Internet service from computer media at his residence and/or could easily travel to Lois Bigler's residence to use her computer media.

46. As noted above, the bigblue8992@yahoo.com Dropbox account had an account name of "Big Jay", and the bigblue8992@yahoo.com Yahoo email account had an account name of "J Big". Based on my training and experience, I know that individuals sometimes use the first initials of their first or last names as nicknames or aliases.
47. On February 17, 2017, the United States District Court for the Southern District of Ohio authorized a search warrant for information associated with the account bigblue8992@gmail.com that is stored at premises controlled by Google Inc. Google Inc. provided records in response to the search warrant on or around February 21, 2017. Review of the records identified that the user of the email account had received approximately 34 email messages from the email address no-reply@dropboxmail.com between the approximate time period of October 3, 2016 and February 12, 2017. These email messages indicated that the user of the bigblue8992@gmail.com email address had established a Dropbox account on or around October 3, 2016. The messages also indicated that the account user had linked an iPad to his/her Dropbox account on or around November 5, 2016. The account user received an email message on or around February 12, 2016, indicating that his Dropbox account had reached its maximum storage capacity.
48. Also on February 17, 2017, the United States District Court for the Southern District of Ohio authorized search warrants for the following: (1) the residential property located at 104 Virginia Avenue, Dayton, Ohio, 45410; (2) the residential property located at 105 Virginia Avenue, Dayton, Ohio, 45410; and (3) a 2000 Saturn SL1 bearing Ohio license plate AXN4197, silver in color. Agents and officers of the FBI and Dayton Police Department executed these warrants on February 21, 2017. Among other items, an iPad was seized from 105 Virginia Avenue; an Apple All-in-One computer was seized from 104 Virginia Avenue, and a Motorola cellular telephone was seized from the Saturn.
49. During the execution of the search warrant for 105 Virginia Avenue, agents encountered Lois Bigler and Donald Bigler. Lois Bigler and Donald Bigler consented to be interviewed. In summary, Lois Bigler and Donald Bigler provided the following information (among other information):
 - a. Lois Bigler and Donald Bigler resided at 105 Virginia Avenue. Jason Bigler was Lois Bigler's and Donald Bigler's son, and he resided at 104 Virginia Avenue.
 - b. Jason Bigler came over to Lois Bigler's and Donald Bigler's residence a few times per week to use their Apple All-in-One computer.
 - c. Lois Bigler had given Jason Bigler her iPad approximately one year ago.

50. During the execution of the search warrants for 104 Virginia Avenue and the 2000 Saturn SL1, agents encountered Jason Bigler. After being advised of his Miranda rights, Jason Bigler consented to be interviewed. In summary, Jason Bigler provided the following information (among other information):
- a. Jason Bigler resided at 105 Virginia Avenue, and his parents resided at 104 Virginia Avenue.
 - b. The Motorola cellular telephone seized from the Saturn was his telephone. The telephone number for this device was 937-304-4995 (the telephone number noted in the subscriber information for the bigblue8992@yahoo.com and bigblue8992@gmail.com email accounts, as detailed above).
 - c. Jason Bigler used the Apple All-in-One computer at his parents' residence to conduct Internet searches, send and receive emails, and help his parents with various computer activities. He also currently had Lois Bigler's iPad in his house. Jason Bigler had used the iPad for the past approximately one and a half years to play games and check his email accounts.
 - d. Jason Bigler initially denied that he could access the wireless Internet service at his parents' residence from his residence. Jason Bigler later acknowledged that he could in fact access the Internet service from his residence and had done so on a number of occasions.
 - e. Jason Bigler used the email addresses bigday@zoomtown.com, bigblue8992@yahoo.com, and bigblue8992@gmail.com.
 - f. When asked if he used any Dropbox accounts, Jason Bigler responded that he did not want to answer the question. When asked if he had viewed child pornography on any of the computer devices, Jason Bigler again responded that he did not want to answer the question. Jason Bigler terminated the interview shortly thereafter.
51. Based on all of the information noted above, I submit that it is reasonable to believe that Jason Bigler is the user of the bigblue8992@yahoo.com and bigblue8992@gmail.com Dropbox accounts and the bigblue8992@yahoo.com and bigblue8992@gmail.com email accounts. I also submit that it is reasonable to believe that the bigblue8992@gmail.com Dropbox account contains evidence of the Jason Bigler's child pornography offenses.

Evidence Available on Dropbox Accounts

52. Dropbox and other cloud storage services provide a means that individuals can use to store files. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.

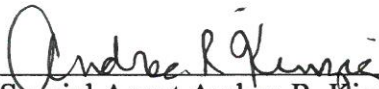
53. Based on information received from Dropbox Inc., I know that Dropbox Inc. maintains basic subscriber information for its users, including user names, email addresses, and the dates that they established their accounts. Dropbox Inc. also maintains payment information, including credit card numbers, when payments are made on the accounts. Such information can provide material evidence regarding individuals involved in child pornography offenses, because this information can help identify the subjects and determine what aliases and email accounts they utilize. In addition, the dates that the accounts were established can help in identifying the length of time that the criminal activities transpired.
54. In addition to maintaining the files themselves, Dropbox Inc. also maintains files documenting various activities associated with its accounts. One such file is entitled "uploadlog.html". This file maintains information about the account name, computer name, and dates that files were uploaded, deleted, and modified. Such information provides material evidence to child pornography investigations, as the information helps identify the computer devices utilized by the subjects and when and how the files were received.
55. Another file maintained by Dropbox Inc. for its accounts is entitled "auth.txt". This file maintains logs of IP addresses and devices utilized to access the account. Such information is important to child pornography investigations because it helps to establish the subjects' identities, what computer devices are utilized, where the subjects' computers are located, and when the criminal activities transpired.
56. A file entitled "links.txt" is another example of a file maintained by Dropbox Inc. for its accounts. This file maintains information about files being shared by the user. In cases involving the trading of child pornography, information about the shared files can be useful in helping to identify the subjects' trading activities.
57. Dropbox Inc. maintains various information about the settings for its users' accounts. Such settings include information about computers and other devices linked to the accounts. Information about what computers and devices are utilized by the subjects is again materially important to child pornography investigations.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

58. I anticipate executing the requested warrant for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

59. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the following criminal offenses may be located in the account described in Attachment A: receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2)(B) & (b)(1) and 2252A(a)(2); and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) & (b)(2) and 2252A(a)(5)(B).
60. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.
61. Because the warrant for the account described in Attachment A will be served on Dropbox Inc., who will then compile the requested records at times convenient to that entity, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 23rd of February 2017


Michael J. Newman
UNITED STATES MAGISTRATE JUDGE

